# DEVICE AND METHOD FOR CALCULATING A RESULT OF A MODULAR EXPONENTIATION


## ABSTRACT

In a device for calculating a result of a modular exponentiation, the Chinese Residue Theorem (CRT) is used, wherein two auxiliary exponentiations are calculated using two auxiliary exponents and two sub-moduli. In order to improve the safety of the RSA CRT calculations against cryptographic attacks, a randomization of the auxiliary exponents and/or a change of the sub-moduli are performed. Thus, there is a safe RSA decryption and RSA encryption, respectively, by means of the calculating time efficient Chinese Residue Theorem.